

Microsoft.SC-500.v2026-09-07.q39

Exam Code:	SC-500
Exam Name:	Implementing End-to-End Security Controls for Cloud and AI Workloads
Certification Provider:	Microsoft
Free Question Number:	39
Version:	v2026-09-07
# of views:	108
# of Questions views:	390
https://www.freecram.net/torrent/Microsoft.SC-500.v2026-09-07.q39.html	

NEW QUESTION: 1

Case Study 1 - Contoso, Ltd.

Overview

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso has a hybrid environment that contains on-premises servers connected to Azure, a Microsoft 365 E5 subscription, and an Azure subscription named Sub1.

Existing Environment. Microsoft Entra tenant

Contoso has a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	AI Administrator
Admin3	Privileged Role Administrator
User1	None

Existing Environment. On-premises environment

The on-premises network contains an Active Directory Domain Services (AD DS) forest that syncs with contoso.com. The forest contains a server named Server1 that runs Windows Server.

Existing Environment. Azure subscription

Sub1 contains the storage accounts shown in the following table.

Name	Azure region	Performance	Premium account type
storage1	West US	Standard	Not applicable
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US	Premium	Page blobs

Sub1 contains the virtual networks shown in the following table.

Name	Azure region	Subnet
VNet1	West US	Subnet1, Subnet2
VNet2	East US	Subnet3
VNet3	West US	Subnet4

Sub1 contains the virtual machines shown in the following table.

Name	Connected to	Network security group (NSG)
VM1	Subnet1	NSG1
VM2	Subnet2	NSG2
VM3	Subnet3	NSG3
VM4	Subnet4	NSG4

The network interface of VM1 is associated with an application security group named ASG1.
Sub1 contains the resources shown in the following table.

Name	Azure region	Description
sql1	West US	Azure SQL server
AKS1	East US	Azure Kubernetes Service (AKS) cluster
Vault1	East US	Azure key vault

Vault1 stores the objects shown in the following table.

Name	Type	Status
Key1	Key	Disabled
Secret1	Secret	Enabled
Certificate1	Certificate	Disabled
Certificate2	Certificate	Enabled

Existing Environment. Privileged Identity Management (PIM) configuration You manage privileged roles by using Privileged Identity Management (PIM). The PIM role settings are configured as shown in the following table.

Setting	State	
	AI Administrator role	Agent ID Developer role
Activation maximum duration (hours)	1 Day(s)	1 Day(s)
Require approval to activate	Enabled	Disabled
Approvers	None	None
Expire eligible assignments after	1 Month(s)	1 Month(s)
Expire active assignments after	15 Day(s)	15 Day(s)

Existing Environment. Microsoft Sentinel configuration

Contoso has a Microsoft Sentinel workspace that contains the following tables.

Name	Tier
DeviceInfo	Analytics
DnsEvents	Analytics

Requirements. Planned changes

Contoso plans to implement the following changes:

- Integrate AKS1 with Vault1.
- Enable Microsoft Entra Kerberos authentication for all supported storage.
- Configure auditing for sql1 by using the Azure portal and store audit logs in a centralized location.

Requirements. Technical requirements

Contoso identifies the following technical requirements:

- Protect Server1 by using file integrity monitoring.
- Protect AKS1 by using Microsoft Defender for Cloud.
- Configure Microsoft Sentinel to retain data for the maximum supported duration without changing the tier.

- Store objects used for authentication and encryption in Vault1 and ensure that Vault1 regenerates the objects every 30 days, whenever possible.

Hotspot Question

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Admin1 must approve requests for the Agent ID Developer role.	☐	☐
Admin2 can approve requests for the AI Administrator role.	☐	☐
Admin3 can assign User1 a two-day active assignment for the Agent ID Developer role.	☐	☐

Answer:

Answer Area

Statements	Yes	No
Admin1 must approve requests for the Agent ID Developer role.	☐	☒
Admin2 can approve requests for the AI Administrator role.	☐	☒
Admin3 can assign User1 a two-day active assignment for the Agent ID Developer role.	☒	☐

NEW QUESTION: 2

You have an Azure key vault named KV1 that uses role-based access control (RBAC) authorization. KV1 stores database connection strings for an Azure App Service web app named App1.

You enable a firewall on KV1 and allow access to KV1 from only the virtual network that contains App1.

You need to ensure that App1 can retrieve secrets from KV1 without using credentials stored in the application configuration.

What should you create?

- A. an access policy for KV1
- B. an app registration for App1
- C. a private endpoint for KV1
- D. a managed identity for App1

Answer: (SHOW ANSWER)

A managed identity enables App1 to authenticate to Azure Key Vault through Microsoft Entra ID without storing or managing application credentials. Because KV1 uses RBAC authorization, the identity must also be assigned an appropriate Key Vault data-plane role, such as Key Vault Secrets User, to retrieve the stored connection strings.

Reference:

<https://learn.microsoft.com/en-us/azure/key-vault/general/authentication>

<https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=portal%2Chttp>

<https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli>

NEW QUESTION: 3

Your organization is deploying several generative AI applications that use Azure AI services.

Security administrators want to ensure that prompts and responses containing sensitive information are identified and monitored before they leave the organization's environment. Which solution should be implemented first?

- A. Azure Firewall Premium
- B. Microsoft Purview Data Loss Prevention (DLP)
- C. Azure Load Balancer
- D. Azure Traffic Manager

Answer: B (LEAVE A REPLY)

Microsoft Purview DLP is designed to discover, classify, and protect sensitive information across Microsoft services. It can help detect sensitive content in AI-related workflows and enforce policies before data is shared externally. Azure Firewall Premium protects network traffic, but it does not provide content-aware DLP capabilities.

NEW QUESTION: 4

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Sentinel workspace.

You have a multi-tier Security Operations Center (SOC) team.

You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.

Solution: You create a playbook.

Does this meet the goal?

- A. Yes
- B. No

Answer: (SHOW ANSWER)

Creating a playbook alone does not ensure that it runs for every newly created incident. A playbook must be invoked by an automation rule or another supported trigger. An automation rule can immediately assign new incidents to the Tier 1 analysts group and apply a triage tag without requiring a playbook.

Reference:

<https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules?tabs=onboarded>

<https://learn.microsoft.com/en-us/azure/sentinel/automation/automation>

NEW QUESTION: 5

You use Azure Virtual Network Manager to manage multiple virtual networks in a network group named Group1.

You discover that the virtual machines in Group1 are accessible from the internet by using TCP port 3389.

You need to block inbound TCP 3389 from the internet across all the virtual networks in Group1.

The solution must minimize administrative effort.

What should you use?

- A. a connectivity configuration
- B. a security admin configuration
- C. a user-defined route (UDR)
- D. a network security group (NSG)

Answer: ([SHOW ANSWER](#))

A security admin configuration in Azure Virtual Network Manager applies centralized security admin rules to all virtual networks in a targeted network group. A deny inbound rule for TCP port

3389 from the internet blocks RDP exposure across Group1 with minimal administrative effort and is evaluated before NSG rules.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network-manager/concept-security-admins>

NEW QUESTION: 6

An organization is evaluating the security of AI-generated content before it is presented to end users. The goal is to detect harmful, unsafe, or policy-violating responses automatically. Which capability should be prioritized?

- A. Deploying additional virtual networks
- B. Content filtering and safety evaluation
- C. Adding more GPUs
- D. Increasing context window size

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

You have an Azure SQL Database logical server named Server1 that contains multiple databases.

The databases contain legacy SQL authentication logins that must no longer be usable for sign-in but must NOT be removed from the databases.

You need to ensure that SQL authentication is denied for connections.

What should you do?

- A. Run create USER ... FROM EXTERNAL PROVIDER on each database.
- B. Create a Conditional Access policy.
- C. Enable Microsoft Entra-only authentication for Server1.
- D. Assign the SQL Server Contributor role to Server1.

Answer: ([SHOW ANSWER](#))

Microsoft Entra-only authentication on an Azure SQL logical server disables SQL authentication for all databases hosted on that server.

Existing SQL authentication logins remain in the databases, but they can no longer be used to establish connections because only Microsoft Entra identities are accepted for authentication.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?view=azuresql&tabs=azure-portal>

NEW QUESTION: 8

A security architect is reviewing an AI application that retrieves enterprise documents using Retrieval-Augmented Generation (RAG). The architect wants to reduce the possibility of unauthorized document exposure. Which control is most important?

- A. Increasing token limits

- B. Implementing document-level access controls
- C. Using larger language models
- D. Enabling autoscaling

Answer: ([SHOW ANSWER](#))

RAG systems retrieve content from external knowledge sources. If document permissions are not enforced, users may gain access to data they are not authorized to view. Document-level authorization ensures retrieval results respect existing security boundaries regardless of model size or scaling configuration.

NEW QUESTION: 9

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have an Azure subscription that contains two virtual machines named VM1 and VM2. Each virtual machine has system-assigned managed identity enabled.

You have an Azure Storage account named storage1. Public access from all networks is enabled for storage1.

You need to ensure that VM1 and VM2 can access storage1.

Solution: You add each virtual machine to a security group, and then add the security group to a role on storage1.

Does this meet the goal?

- A. Yes
- B. No

Answer: ([SHOW ANSWER](#))

A system-assigned managed identity is a Microsoft Entra security principal and can be added to a Microsoft Entra security group. Assigning an appropriate Azure Storage data-access role to that security group grants the managed identities of VM1 and VM2 access to storage1. Group-based permission changes for managed identities can take several hours to become effective because managed identity tokens are cached, but the solution meets the access requirement.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identity-best-practice-recommendations>

NEW QUESTION: 10

Case Study 1 - Contoso, Ltd.

Overview

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso has a hybrid environment that contains on-premises servers connected to Azure, a Microsoft 365 E5 subscription, and an Azure subscription named Sub1.

Existing Environment. Microsoft Entra tenant

Contoso has a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	AI Administrator
Admin3	Privileged Role Administrator
User1	None

Existing Environment. On-premises environment

The on-premises network contains an Active Directory Domain Services (AD DS) forest that syncs with contoso.com. The forest contains a server named Server1 that runs Windows Server.

Existing Environment. Azure subscription

Sub1 contains the storage accounts shown in the following table.

Name	Azure region	Performance	Premium account type
storage1	West US	Standard	Not applicable
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US	Premium	Page blobs

Sub1 contains the virtual networks shown in the following table.

Name	Azure region	Subnet
VNet1	West US	Subnet1, Subnet2
VNet2	East US	Subnet3
VNet3	West US	Subnet4

Sub1 contains the virtual machines shown in the following table.

Name	Connected to	Network security group (NSG)
VM1	Subnet1	NSG1
VM2	Subnet2	NSG2
VM3	Subnet3	NSG3
VM4	Subnet4	NSG4

The network interface of VM1 is associated with an application security group named ASG1.

Sub1 contains the resources shown in the following table.

Name	Azure region	Description
sql1	West US	Azure SQL server
AKS1	East US	Azure Kubernetes Service (AKS) cluster
Vault1	East US	Azure key vault

Vault1 stores the objects shown in the following table.

Name	Type	Status
Key1	Key	Disabled
Secret1	Secret	Enabled
Certificate1	Certificate	Disabled
Certificate2	Certificate	Enabled

Existing Environment. Privileged Identity Management (PIM) configuration You manage privileged roles by using Privileged Identity Management (PIM). The PIM role settings are configured as shown in the following table.

Setting	State	
	AI Administrator role	Agent ID Developer role
Activation maximum duration (hours)	1 Day(s)	1 Day(s)
Require approval to activate	Enabled	Disabled
Approvers	None	None
Expire eligible assignments after	1 Month(s)	1 Month(s)
Expire active assignments after	15 Day(s)	15 Day(s)

Existing Environment. Microsoft Sentinel configuration

Contoso has a Microsoft Sentinel workspace that contains the following tables.

Name	Tier
DeviceInfo	Analytics
DnsEvents	Analytics

Requirements. Planned changes

Contoso plans to implement the following changes:

- Integrate AKS1 with Vault1.
- Enable Microsoft Entra Kerberos authentication for all supported storage.
- Configure auditing for sql1 by using the Azure portal and store audit logs in a centralized location.

Requirements. Technical requirements

Contoso identifies the following technical requirements:

- Protect Server1 by using file integrity monitoring.
- Protect AKS1 by using Microsoft Defender for Cloud.
- Configure Microsoft Sentinel to retain data for the maximum supported duration without changing the tier.
- Store objects used for authentication and encryption in Vault1 and ensure that Vault1 regenerates the objects every 30 days, whenever possible.

Hotspot Question

You need to configure Server1 to meet the technical requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Install on Server1:

The Azure Monitor Agent

The Azure File Sync agent

Microsoft Entra Connect Sync

The Azure Connected Machine agent

A Microsoft Defender for Endpoints onboarding package

Deploy to Sub1:

Azure File Sync

A Log Analytics workspace

An Azure Machine Learning workspace

Defender for Cloud workflow automation

Answer:

Answer Area

Install on Server1:

- The Azure Monitor Agent
- The Azure File Sync agent
- Microsoft Entra Connect Sync
- The Azure Connected Machine agent
- A Microsoft Defender for Endpoints onboarding package**

Deploy to Sub1:

- Azure File Sync
- A Log Analytics workspace**
- An Azure Machine Learning workspace
- Defender for Cloud workflow automation

NEW QUESTION: 11

You have an Azure subscription named Sub1 that contains multiple virtual machines.

You have a Microsoft 365 E5 subscription that contains devices onboarded to Microsoft Defender for Endpoint.

You have an on-premises datacenter that contains multiple servers.

You plan to onboard all existing and future on-premises servers to Azure Arc.

You need to ensure that the Azure Arc-enabled servers are protected by using the same security features as the Microsoft 365 devices immediately after the servers are onboarded. The solution must minimize administrative effort.

What should you do?

- A.** Onboard each server to Microsoft Defender for Endpoint by using Group Policy.
- B.** Onboard each server to Microsoft Defender for Endpoint by using a local installation script.
- C.** For Sub1, enable the Microsoft Defender for Servers plan in Microsoft Defender for Cloud.
- D.** Configure an Azure Policy assignment.

Answer: (SHOW ANSWER)

Microsoft Defender for Servers extends Microsoft Defender for Endpoint protection to Azure Arc- enabled on-premises servers. Enabling the plan on the Azure subscription to which the Arc- enabled servers are onboarded provides centralized deployment and management of the Defender for Endpoint integration for existing and newly onboarded servers, minimizing manual administration.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-overview>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/connect-azure-subscription>

NEW QUESTION: 12

Hotspot Question

You have a Microsoft Sentinel workspace named Workspace1.

You hire a security consultant. You provide the consultant with a guest account named User1 in your Microsoft Entra tenant.

You need to enable User1 to assign incidents in Workspace1.

Which roles should you assign to User1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Microsoft

Microsoft Entra role:

Directory Reader

Security Administrator

Security Reader

Azure role:

Microsoft Sentinel Contributor

Microsoft Sentinel Reader

Microsoft Sentinel Responder

Answer:

Answer Area

Microsoft

Microsoft Entra role:

Directory Reader

Security Administrator

Security Reader

Azure role:

Microsoft Sentinel Contributor

Microsoft Sentinel Reader

Microsoft Sentinel Responder

NEW QUESTION: 13

Drag and Drop Question

You have an Azure key vault named KV1 that uses role-based access control (RBAC) for data plane authorization.
You have a user named User1 and an Azure App Service web app named App1 that has a system-assigned managed identity.
You need to configure authorization to meet the following requirements:

- App1 must be able to retrieve secrets from KV1.
- User1 must manage the KV1 settings without accessing secret values.

The solution must follow the principle of least privilege.

Which role should you assign to each identity for KV1? To answer, drag the appropriate roles to the correct identities. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles	Answer Area
Key Vault Administrator	User1:
Key Vault Contributor	App1:
Key Vault Secrets Officer	
Key Vault Secrets User	

Answer:

Roles	Answer Area
Key Vault Administrator	User1: Key Vault Contributor
Key Vault Contributor	App1: Key Vault Secrets User
Key Vault Secrets Officer	
Key Vault Secrets User	

NEW QUESTION: 14

You have a Microsoft Copilot Studio agent.

A Microsoft Power Platform administrator configures external threat detection for the agent by using a Microsoft Entra application.

You need to ensure that real-time protection is enabled during agent runtime.

What should you do in the Microsoft Defender portal?

- A. Configure Microsoft Defender for Cloud Apps session policies.
- B. Connect the Microsoft 365 app connector.
- C. Enable Global Secure Access for Agents.
- D. From Microsoft Sentinel, configure the Microsoft Purview data connector.

Answer: (SHOW ANSWER)

In the Microsoft Defender portal, connecting the Microsoft 365 app connector is part of enabling Microsoft Defender real-time protection integration for Microsoft Copilot Studio agents. The Microsoft Entra application configuration performed by the Power Platform administrator establishes the agent integration, while the connector enables the related protection output, alerts, and incidents to surface in Microsoft Defender.

Reference:

<https://learn.microsoft.com/en-us/defender-cloud-apps/real-time-agent-protection-during-runtime>

<https://learn.microsoft.com/en-us/defender-xdr/security-for-ai/ai-agent-detection-protection>

NEW QUESTION: 15

An organization wants to prevent accidental deployment of AI resources in regions that are not approved by regulatory requirements.

Which Azure governance feature should be used?

- A. Azure Policy

- B. Azure Advisor
- C. Azure Monitor
- D. Azure Automation

Answer: ([SHOW ANSWER](#))

Azure Policy can enforce compliance requirements by restricting resource deployments to approved regions. Policies can deny noncompliant deployments before resources are created.

Azure Advisor provides recommendations, while Azure Monitor and Automation focus on monitoring and operational tasks rather than governance enforcement.

NEW QUESTION: 16

You have an Azure subscription that contains a resource group named RG1.

RG1 contains a Microsoft Security Copilot deployment that is integrated with a Microsoft Sentinel workspace named Workspace1.

Analysts use the Security Copilot standalone experience to retrieve incidents by using the Microsoft Sentinel plugin.

A user named User1 can sign in to Security Copilot but cannot retrieve incidents from Workspace1. You verify that User1 has only the Security Copilot Contributor role.

You need to ensure that User1 can retrieve the incidents. The solution must follow the principle of least privilege and NOT require any configuration changes to Security Copilot.

Which role should you assign to User1?

- A. the Security Reader role in Microsoft Entra
- B. the Microsoft Sentinel Reader role for Workspace1
- C. the Security Copilot Owner role
- D. the Security Administrator role in Microsoft Entra
- E. the Contributor role in Azure for RG1

Answer: ([SHOW ANSWER](#))

The Security Copilot Contributor role permits User1 to use the Security Copilot platform, but it does not grant access to Microsoft Sentinel data. Assigning the Microsoft Sentinel Reader role at the Workspace1 scope grants read access to the workspace incidents through the Microsoft Sentinel plugin while avoiding broader security administration or resource modification privileges.

Reference:

<https://learn.microsoft.com/en-us/copilot/security/authentication>

Valid SC-500 Dumps shared by EduDump.com for Helping Passing SC-500 Exam! EduDump.com now offer the **newest SC-500 exam dumps**, the EduDump.com SC-500 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-500 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-500/premium/> (136 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 17

You are configuring a new Microsoft Sentinel workspace named Workspace1.

You have an external IT Service Management (ITSM) system that is NOT supported by any Microsoft Sentinel solutions in Azure Marketplace.

You need to ensure that Workspace1 creates service tickets in the ITSM system for all new security incidents.

What should you create?

- A. a playbook
- B. a workbook
- C. a watchlist
- D. an analytics rule

Answer: ([SHOW ANSWER](#))

A Microsoft Sentinel playbook is an Azure Logic Apps workflow that automates response actions when incidents are created. It can integrate with an external ITSM system through an available connector or API call to create service tickets for new security incidents, even when no packaged Microsoft Sentinel solution exists for that system.

Reference:

<https://learn.microsoft.com/en-us/azure/sentinel/automation/integrations>

<https://learn.microsoft.com/en-us/azure/sentinel/automation/automation>

<https://learn.microsoft.com/en-us/azure/sentinel/automation/playbook-recommendations>

NEW QUESTION: 18

Case Study 2 - Fabrikam, Inc.

Overview

Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore.

Existing Environment. Network environment

The on-premises network contains a datacenter in each office.

Existing Environment. Cloud environment

Fabrikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses.

All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

Name	Type	Microsoft Entra role	Azure role assignment for Sub1
Admin1	User	Privileged Authentication Administrator	Resource Policy Contributor
Admin2	User	Compliance Administrator	User Access Administrator
Admin3	User	Authentication Administrator	Contributor
Admin4	User	Global Administrator	None
User1	User	None	Reader
AKS1	System-assigned managed identity	None	None
ID1	User-assigned managed identity	None	None

The tenant contains the groups shown in the following table.

Name	Type	Role assignments allowed
Group1	Security	Yes
Group2	Security	No
Group3	Microsoft 365	Yes
Group4	Microsoft 365	No

All devices are enrolled in Microsoft Intune.

Existing Environment. Sub1 Resources

Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

Name	Description	Location
SQLServer1	Azure SQL Database logical server	East US
SQLdb1	Database on SQLServer1	East US
VM1	Virtual machine	East US
AKS1	Azure Kubernetes Service (AKS) cluster	East US
Registry1	Azure container registry	East US
storage1	Storage account	East US
AKV1	Azure key vault	East US

SQLServer1 uses Microsoft SQL Server authentication.

Sub1 has an Azure Web Application Firewall (WAF) named WAF1 that has the following types of rule sets:

- Bot Manager 1.1
- Azure-managed Default Rule Set (DRS)

Sub1 has the following compliance standards assigned in Microsoft Defender for Cloud:

- NIST SP 800-53 Rev. 4
- Microsoft cloud security benchmark (MCSB)
- System and Organization Controls (SOC) 2 Type 2

Existing Environment. Sub2 Resources

Sub2 contains a resource group named RG2.

Planned Changes and Requirements. Planned Changes

Fabrikam plans to implement the following changes:

- Deploy the following key vaults to RG1:
 - * AKV2 in the West Europe Azure region
 - * AKV3 in the Central US Azure region
 - * AKV4 in the East US Azure region
- Deploy the following key vaults to RG2:
 - * AKV5 in the East US region
- Configure VM1 to read data from storage1.
- Create function apps that have the following hosting plans:
 - * Fa1: Flex Consumption hosting plan
 - * Fa2: Consumption hosting plan
 - * Fa3: Dedicated hosting plan
- For WAF1, implement rate limiting rules based on the request location.
- Enable the NIST SP 800-53 Rev. 5 compliance standard in Defender for

Cloud.

- Create a new storage account named storage2 that supports Azure Table storage.
- Enforce multifactor authentication (MFA) when database administrators access SQLdb1.
- Implement ExpressRoute circuits to the on-premises network as shown in the following table.

Name	Location	Deployment type
ER1	West Europe	ExpressRoute with a connectivity provider
ER2	West Europe	ExpressRoute Metro with a connectivity provider
ER3	East US	ExpressRoute Direct
ER4	Southeast Asia	ExpressRoute Metro Direct

- For RG1, create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups.

Planned Changes and Requirements. Technical Requirements

Fabrikam has the following technical requirements:

- If VM1 is deleted, the permissions for VM1 must be removed automatically.
- The AKS1 managed identity must only be able to pull images from Registry1.
- The ID1 managed identity must be able to push images to and pull images from Registry1.
- All the data in the storage accounts must be encrypted by using Fabrikam-managed keys.
- All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits.
- ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.

You need to implement the function apps to meet the technical requirements. Which apps should you include in the implementation?

- A. Fa1 and Fa2 only
- B. Fa2 and Fa3 only
- C. Fa1 and Fa3 only
- D. Fa1, Fa2, and Fa3

Answer: (SHOW ANSWER)

Flex Consumption and Dedicated hosting plans support outbound virtual network integration, which enables function app traffic to reach on-premises resources across ExpressRoute connections. The Consumption hosting plan does not support virtual network integration and therefore cannot meet the outbound routing requirement. For Flex Consumption, all traffic is routed through the integrated virtual network; for Dedicated hosting, outbound routing through the virtual network can be enabled to use the ExpressRoute path.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-functions/functions-networking-options?tabs=azure-portal&pivots=flex-consumption-plan>

NEW QUESTION: 19

A company wants administrators to receive just-in-time access to privileged Azure roles instead of maintaining permanent assignments. Which Microsoft Entra feature should be implemented?

- A. Dynamic groups
- B. Privileged Identity Management (PIM)
- C. Access Packages
- D. Self-service password reset

Answer: ([SHOW ANSWER](#))

Privileged Identity Management enables eligible role assignments that can be activated when needed, often requiring approval, MFA, or justification. This reduces standing privileges and limits exposure. Dynamic groups and Access Packages address different identity governance scenarios, while password reset focuses on account recovery.

NEW QUESTION: 20

You have multiple Microsoft Security Copilot workspaces.
A user named User1 accesses Security Copilot by using the default workspace.
You create a new workspace named Workspace1 and assign a capacity to Workspace1.
You plan to route Security Copilot agent traffic to Workspace1.
You need to ensure that User1 can use embedded experiences without errors.
What should you do before switching to Workspace1?

- A. Add User1 to Workspace1.
- B. Assign User1 the Security Operator role in Microsoft Entra.
- C. Disassociate the capacity from the default workspace.
- D. Create a new capacity for Workspace1.

Answer: ([SHOW ANSWER](#))

Access to Microsoft Security Copilot capabilities is controlled through workspace role assignments. Before agent traffic is routed to Workspace1, User1 must be added to that workspace with the required Security Copilot access so the user can continue using agent capabilities in embedded experiences without authorization errors.

Reference:

<https://learn.microsoft.com/en-us/copilot/security/authentication>

<https://learn.microsoft.com/en-us/copilot/security/faq-security-copilot>

NEW QUESTION: 21

You have an Azure subscription named Sub1 that contains a storage account named storage1.
Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has on-upload malware scanning enabled for a monthly cap of 10,000 GB per storage account.
You use a Microsoft Sentinel workspace to monitor security events on all Azure resources.
You need to configure storage1 to use a malware scanning cap of 2,000 GB per month.
What should you do?

- A. Enable the Override Defender for Storage subscription-level settings for storage1.

- B.** From Microsoft Sentinel, modify the data collection rule (DCR) to restrict log ingestion from storage1.
- C.** Modify the malware scanning configuration of Sub1.
- D.** From the Microsoft Sentinel workspace, modify the daily cap.

Answer: ([SHOW ANSWER](#))

Defender for Storage settings can be overridden for an individual storage account when the subscription-level configuration applies a different malware scanning cap. Enabling the override for storage1 allows its on-upload malware scanning monthly cap to be changed to 2,000 GB while the subscription-level 10,000-GB setting continues to apply to other storage accounts.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-azure-portal-enablement?tabs=enable-subscription>

NEW QUESTION: 22

You have a Microsoft Entra tenant that has the following configurations:

- User consent for applications is disabled.
- Only administrators can grant permissions to applications.

You register an application named App1 that uses delegated Microsoft Graph permissions.

You need to configure App1 to meet the following requirements:

- Enable user sign-ins without interactive consent prompts.
- Enable App1 to access Microsoft Graph on behalf of the signed-in user.

What should you do?

- A.** Configure enterprise applications to require user assignment and assign users to App1.
- B.** Modify the app registration to use application permissions instead of delegated permissions.
- C.** Add the required delegated Microsoft Graph permissions to the app registration and rely on user consent during sign-in.
- D.** Grant admin consent to App1 for the required delegated permissions.

Answer: ([SHOW ANSWER](#))

Admin consent grants the required delegated Microsoft Graph permissions on behalf of the tenant. App1 can then call Microsoft Graph in the context of a signed-in user without requiring individual users to respond to consent prompts, which is necessary because user consent is disabled.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?pivots=portal>

<https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-configure-app-access-web-apis>

NEW QUESTION: 23

You have a Microsoft Sentinel workspace.

You need to collect Windows security events from 200 Azure virtual machines that run Windows Server. The solution must meet the following requirements:

- Use direct agent-based data collection from each virtual machine.
- Use a supported agent for new virtual machine deployments.

Which Microsoft Sentinel connector should you use?

- A.** Windows Forwarded Events

- B. Windows Security Events via AMA
- C. Security Events via Legacy Agent
- D. Syslog via AMA
- E. Azure Resource Graph

Answer: (SHOW ANSWER)

The Windows Security Events via AMA connector uses the Azure Monitor Agent to collect Windows security events directly from Azure virtual machines and send them to the Microsoft Sentinel SecurityEvent table. Azure Monitor Agent is the supported agent for new guest operating system data collection deployments, replacing legacy agent-based collection.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-windows-events>

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-overview>

NEW QUESTION: 24

Case Study 2 - Fabrikam, Inc.

Overview

Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore.

Existing Environment. Network environment

The on-premises network contains a datacenter in each office.

Existing Environment. Cloud environment

Fabrikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses.

All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

Name	Type	Microsoft Entra role	Azure role assignment for Sub1
Admin1	User	Privileged Authentication Administrator	Resource Policy Contributor
Admin2	User	Compliance Administrator	User Access Administrator
Admin3	User	Authentication Administrator	Contributor
Admin4	User	Global Administrator	None
User1	User	None	Reader
AKS1	System-assigned managed identity	None	None
ID1	User-assigned managed identity	None	None

The tenant contains the groups shown in the following table.

Name	Type	Role assignments allowed
Group1	Security	Yes
Group2	Security	No
Group3	Microsoft 365	Yes
Group4	Microsoft 365	No

All devices are enrolled in Microsoft Intune.

Existing Environment. Sub1 Resources

Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

Name	Description	Location
SQLServer1	Azure SQL Database logical server	East US
SQLdb1	Database on SQLServer1	East US
VM1	Virtual machine	East US
AKS1	Azure Kubernetes Service (AKS) cluster	East US
Registry1	Azure container registry	East US
storage1	Storage account	East US
AKV1	Azure key vault	East US

SQLServer1 uses Microsoft SQL Server authentication.

Sub1 has an Azure Web Application Firewall (WAF) named WAF1 that has the following types of rule sets:

- Bot Manager 1.1
- Azure-managed Default Rule Set (DRS)

Sub1 has the following compliance standards assigned in Microsoft Defender for Cloud:

- NIST SP 800-53 Rev. 4
- Microsoft cloud security benchmark (MCSB)
- System and Organization Controls (SOC) 2 Type 2

Existing Environment. Sub2 Resources

Sub2 contains a resource group named RG2.

Planned Changes and Requirements. Planned Changes

Fabrikam plans to implement the following changes:

- Deploy the following key vaults to RG1:

- * AKV2 in the West Europe Azure region
- * AKV3 in the Central US Azure region
- * AKV4 in the East US Azure region
- Deploy the following key vaults to RG2:
- * AKV5 in the East US region
- Configure VM1 to read data from storage1.
- Create function apps that have the following hosting plans:
- * Fa1: Flex Consumption hosting plan
- * Fa2: Consumption hosting plan
- * Fa3: Dedicated hosting plan
- For WAF1, implement rate limiting rules based on the request location.
- Enable the NIST SP 800-53 Rev. 5 compliance standard in Defender for Cloud.
- Create a new storage account named storage2 that supports Azure Table storage.
- Enforce multifactor authentication (MFA) when database administrators access SQLdb1.
- Implement ExpressRoute circuits to the on-premises network as shown in the following table.

Name	Location	Deployment type
ER1	West Europe	ExpressRoute with a connectivity provider
ER2	West Europe	ExpressRoute Metro with a connectivity provider
ER3	East US	ExpressRoute Direct
ER4	Southeast Asia	ExpressRoute Metro Direct

- For RG1, create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups.
- Planned Changes and Requirements. Technical Requirements
- Fabrikam has the following technical requirements:
- If VM1 is deleted, the permissions for VM1 must be removed automatically.
 - The AKS1 managed identity must only be able to pull images from Registry1.
 - The ID1 managed identity must be able to push images to and pull images from Registry1.
 - All the data in the storage accounts must be encrypted by using Fabrikam-managed keys.
 - All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits.

- ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.

You need to implement the planned change for SQLdb1.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.** Create a compliance policy.
- B.** Configure Microsoft Entra authentication for SQLServer1.
- C.** Create a Conditional Access policy.
- D.** Configure Federated client identity for SQLdb1.
- E.** Configure a user-assigned managed identity for SQLdb1

Answer: ([SHOW ANSWER](#))

Microsoft Entra authentication must be configured for SQLServer1 so database administrators can authenticate to Azure SQL Database by using Microsoft Entra identities. A Conditional Access policy can then target Azure SQL Database and require multifactor authentication when administrators connect to SQLdb1.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?view=azuresql&tabs=azure-portal>

<https://learn.microsoft.com/en-us/azure/azure-sql/database/conditional-access-configure?view=azuresql>

NEW QUESTION: 25

Hotspot Question

You have an Azure subscription that contains the following resources:

- An Azure SQL Database logical server named Server1 that contains a database named DB1
- An Azure SQL Managed Instance named Instance1 that contains a database named DB2

You need to configure database auditing. The solution must meet the following requirements:

- Ensure that audit data is centrally available in a location that supports for KQL queries.
- Minimize ongoing administrative effort as additional databases are added.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Auditing scope:

Enable on each database.
Enable on each server or instance.
Enable on a per-table basis for each database.

Auditing destination:

An Azure Event Hubs namespace
An Azure Storage account
A Log Analytics workspace

Answer:

Answer Area

Auditing scope:

Enable on each database.
Enable on each server or instance.
Enable on a per-table basis for each database.

Auditing destination:

An Azure Event Hubs namespace
An Azure Storage account
A Log Analytics workspace

NEW QUESTION: 26

You have a Microsoft Sentinel workspace named Workspace1.

You have 100 on-premises servers that run Linux and have the Azure Monitor Agent installed.

You need to collect Syslog events from the Linux servers. The solution must meet the following requirements:

- Ensure that filtering occurs before data is written to Workspace1.
- Reduce ingestion costs by excluding low-value Syslog messages.

What should you include in the solution?

- A.** an Advanced Security Information Model (ASIM) parser
- B.** a data collection rule (DCR)
- C.** an analytics rule
- D.** a table-level filter and split transformation

Answer: B (LEAVE A REPLY)

A data collection rule defines the Syslog facilities and severity levels that the Azure Monitor Agent collects from the Linux servers and sends to Workspace1. By excluding low-value messages in the rule, unwanted events are filtered before storage in the Log Analytics workspace, reducing data ingestion costs.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-syslog>

<https://learn.microsoft.com/en-us/azure/sentinel/connect-cef-syslog-ama?tabs=portal>

NEW QUESTION: 27

You have an Azure subscription named Sub1. Sub1 contains 20 virtual machines that run Windows Server.

Sub1 has the Microsoft Defender for Cloud Defender Cloud Security Posture Management (CSPM) plan enabled.

You need to ensure that all the virtual machines are scanned automatically for known security flaws and misconfigurations.

What should you use?

- A. attack path analysis
- B. Microsoft cloud security benchmark (MCSB)
- C. cloud security explorer
- D. just-in-time (JIT) VM access
- E. vulnerability assessment on the virtual machines

Answer: (SHOW ANSWER)

Vulnerability assessment on the virtual machines uses Microsoft Defender Vulnerability Management to automatically discover known vulnerabilities and security configuration weaknesses on the Windows Server virtual machines. With Defender CSPM, agentless vulnerability scanning provides this assessment without requiring a scanning agent to be installed on each machine.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vm>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-defender-vulnerability-management>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-agentless-data-collection>

NEW QUESTION: 28

You have an Azure subscription named Sub1 that contains an Azure Database for PostgreSQL instance. Sub1 has Microsoft Defender for Cloud enabled.

You need to configure Microsoft Defender for Databases to minimize costs.

Which Defender plan should you enable?

- A. Microsoft Defender for Servers
- B. Microsoft Defender for Open-Source Relational Databases
- C. Microsoft Defender for SQL Servers on Machines
- D. Microsoft Defender for Azure SQL Databases
- E. Microsoft Defender for Storage

Answer: (SHOW ANSWER)

Microsoft Defender for Open-Source Relational Databases provides threat protection specifically for Azure Database for PostgreSQL. Enabling only this database-specific plan minimizes costs because Defender for Databases offerings are priced separately, and no unrelated resource protection plans are required.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-databases-introduction>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-databases-overview>

NEW QUESTION: 29

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft Sentinel workspace.

You have a multi-tier Security Operations Center (SOC) team.

You need to ensure that all new security incidents are assigned immediately to the Tier 1 analysts group and flagged for triage.

Solution: You create a hunting query.

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

A hunting query is used to investigate threats and identify suspicious activity; it does not automatically assign newly created incidents or flag them for triage. An automation rule triggered when an incident is created is required to assign incidents to the Tier 1 analysts group and apply a triage tag or task automatically.

Reference:

<https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules?tabs=defender-portal%2Conboarded>

NEW QUESTION: 30

Drag and Drop Question

You have a Microsoft Entra tenant.

You need to implement passwordless authentication. The solution must meet the following requirements:

- Users can sign in without a password by using a mobile device.
- New users that sign in for the first time must use a helpdesk-issued sign-in method that expires.

Which authentication method should you enable for each requirement? To answer, drag the appropriate methods to the correct requirements. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

The screenshot shows a drag-and-drop interface for selecting authentication methods. On the left, under 'Methods', there are five options: Hardware OATH tokens, Microsoft Authenticator, SMS, Temporary Access Pass, and Voice call. On the right, under 'Answer Area', there are two requirements: 'Passwordless sign-in:' and 'First-time sign-in for new users:'. Each requirement has a corresponding empty box for dropping a method. A watermark 'freecram.net' and the Microsoft logo are visible across the interface.

Answer:

Methods	Answer Area
Hardware OATH tokens	Passwordless sign-in: Microsoft Authenticator
Microsoft Authenticator	
SMS	First-time sign-in for new users: Temporary Access Pass
Temporary Access Pass	
Voice call	



NEW QUESTION: 31

You have an Azure Storage account named storage1 that hosts a blob container named container1.

You have an Azure Functions app named app1 that uses a managed identity.

You need to configure app1 to read, write, and delete blobs in container1. The solution must follow the principle of least privilege.

What should you do?

- A. Assign the Storage Account Contributor role to the managed identity of app1 at the scope of storage1.
- B. Assign the Storage Blob Delegator role to the managed identity of App1 at the scope of container1.
- C. Assign the Owner role to the managed identity of App1 at the scope of container1.
- D. Assign the Storage Blob Data Contributor role to the managed identity of App1 at the scope of container1.

Answer: D (LEAVE A REPLY)

The Storage Blob Data Contributor role grants permissions to read, write, and delete blob data.

Assigning it to the managed identity at the scope of container1 limits access to only the required container, satisfying the principle of least privilege.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access?tabs=portal>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Valid SC-500 Dumps shared by EduDump.com for Helping Passing SC-500 Exam! EduDump.com now offer the **newest SC-500 exam dumps**, the EduDump.com SC-500 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-500 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-500/premium/> (136 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 32

Drag and Drop Question

You have an Azure subscription named Sub1 that contains a virtual network named VNet1.

VNet1 contains multiple virtual machines, including two virtual machines named VM1 and VM2.
Sub1 is linked to a Microsoft Entra tenant named contoso.com.
A partner company has an Azure subscription named Sub2 that contains a virtual network named VNet2. VNet2 contains a virtual machine named VM3.
Sub2 is linked to a Microsoft Entra tenant named fabrikam.com.
VM1 and VM2 contain data used by an application that runs on VM3.
You need to ensure that VM3 can access VM1 and VM2. The solution must deny VM3 access to any other resources in Sub1.
What should you configure on each virtual network? To answer, drag the components to the correct virtual networks. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Components

An Azure Private Link service

An Azure VPN gateway

A private endpoint

A service endpoint

VNet peering

Answer Area

VNet1:

VNet2:

Components

An Azure Private Link service

An Azure VPN gateway

A private endpoint

A service endpoint

VNet peering

Answer Area

VNet1:

An Azure Private Link service

VNet2:

A private endpoint

NEW QUESTION: 33

Drag and Drop Question

You have an Azure virtual network named VNet1 that contains three subnets named Subnet1, Subnet2, and Subnet3. A single network security group (NSG) named NSG1 is associated with all the subnets. You have the following virtual machines:

- VM1 on Subnet1
- VM2 on Subnet2

- VM3 on Subnet3

You create two application security groups named ASG1 and ASG2. VM2 is a member of ASG1, and VM3 is a member of ASG2. You need to ensure that only VM2 can connect to VM3. The solution must continue to work if the private IP address of VM2 changes. How should you configure the inbound rule on NSG1? To answer, drag the settings to the correct configurations. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Settings	Answer Area
ASG1	Source:
ASG2	Destination:
IP address of VM1	
IP address of VM2	
IP address of VM3	
VirtualNetwork	

Answer:

Settings	Answer Area
ASG1	Source: ASG1
ASG2	Destination: ASG2
IP address of VM1	
IP address of VM2	
IP address of VM3	
VirtualNetwork	

NEW QUESTION: 34

You use Microsoft Security Copilot. Security Copilot contributors currently create custom plugins for their own sessions and manage organization-wide custom plugins. You need to prevent the contributors from managing the organization-wide custom plugins. The solution must NOT affect the contributors' ability to create custom plugins for their own sessions.

What should you select in the Plugin settings?

- A. Contributors and Owners at the tenant scope
- B. Owners only at the user scope
- C. Contributors and Owners at the user scope
- D. Owners only at the tenant scope

Answer: ([SHOW ANSWER](#))

Setting tenant-scope custom plugin management to Owners only prevents contributors from adding or managing plugins for the entire organization. Contributors can still create and manage their own session-specific custom plugins because the user-scope permission is not changed.

Reference:

<https://learn.microsoft.com/en-us/copilot/security/manage-plugins?tabs=securitycopilotplugin>

NEW QUESTION: 35

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ContReg1.

You enable content trust for ContReg1.

You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege.

Which two roles should you assign to User1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. AcrQuarantineWriter
- B. Contributor
- C. AcrQuarantineReader
- D. AcrPush
- E. AcrImageSigner

Answer: ([SHOW ANSWER](#))

Creating trusted images in a content trust-enabled Azure Container Registry requires permission to push the image content and permission to sign the image by using Docker Content Trust. The two roles together grant only the required publishing and signing capabilities for trusted container images.

Reference:

<https://learn.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

<https://learn.microsoft.com/en-us/azure/container-registry/container-registry-rbac-built-in-roles-overview?tabs=registries-configured-with-rbac-registry-abac-repository-permissions>

NEW QUESTION: 36

Your organization plans to allow developers to access Azure OpenAI resources. Management wants to ensure that access permissions follow the principle of least privilege. What should you use?

- A. Azure Policy exemptions
- B. Role-Based Access Control (RBAC) roles
- C. Resource locks
- D. Management groups only

Answer: ([SHOW ANSWER](#))

Azure RBAC enables administrators to assign only the permissions required for specific tasks.

Developers can receive limited access to Azure OpenAI resources without granting excessive privileges. Resource locks prevent accidental deletion, while management groups and policy exemptions do not directly enforce least-privilege authorization.

NEW QUESTION: 37

You have a management group named MG1 that contains two subscriptions named Sub1 and Sub2.

Sub1 contains a resource group named RG-Exception and a resource group named RG1 that hosts Microsoft Foundry resources.

You need to assign an Azure policy to force new Foundry deployments in MG1 to use private endpoints. The solution must NOT restrict deployments in RG-Exception.

How should you configure the policy?

- A.** Assign the policy to MG1 and exclude RG-Exception.
- B.** Assign the policy to Sub1 and RG-Exception.
- C.** Assign the policy to MG1 and RG-Exception.
- D.** Assign the policy to Sub1 and exclude RG-Exception.

Answer: ([SHOW ANSWER](#))

Assigning the policy at the MG1 scope enforces the private endpoint requirement for new Microsoft Foundry deployments in all subscriptions and resource groups beneath the management group. Configuring RG-Exception as an excluded scope prevents the policy from restricting deployments in that resource group while maintaining centralized enforcement everywhere else in MG1.

Reference:

<https://learn.microsoft.com/en-us/azure/governance/policy/overview>

<https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>

NEW QUESTION: 38

You have an Azure subscription named Sub1 that contains an Azure Kubernetes Service (AKS) cluster named cluster1 and an Azure container registry named ACR1. Sub1 has Microsoft Defender for Containers enabled, and runtime protection is active on cluster1.

The developers at your company deploy pods that have elevated privileges, and the deployments are created in cluster1.

You need to prevent pods with elevated privileges from being accepted by cluster1.

What should you do?

- A.** Create an Azure policy for cluster1.
- B.** Enable agentless discovery for Kubernetes in Defender for Containers.
- C.** Configure runtime threat protection alerts for privileged container activity.
- D.** Enable vulnerability assessment for images in ACR1.

Answer: ([SHOW ANSWER](#))

Azure Policy for Kubernetes can enforce admission controls on AKS resources. Assigning the built-in policy that disallows privileged containers with the Deny effect prevents new pod deployments configured with elevated privileges from being accepted by cluster1.

Reference:

<https://learn.microsoft.com/en-us/azure/aks/policy-reference>

<https://learn.microsoft.com/en-us/azure/aks/use-azure-policy>

NEW QUESTION: 39

You have an Azure Storage account named storage1 that contains Azure Files shares.

You have an application named App1 that uses a system-assigned managed identity to access the shares.

Administrators access the shares by using storage account keys.

You need to ensure that App1 access the shares without using the storage account keys.

What should you do on storage1?

- A.** Store the storage account access keys in Azure Key Vault and regenerate them periodically.
- B.** Set Allow storage account key access to Disabled.
- C.** Select Default to Microsoft Entra authorization in the Azure portal.
- D.** Assign the Storage File Data Privileged Reader role to the managed identity of App1.

Answer: ([SHOW ANSWER](#))

Assigning the Storage File Data Privileged Reader role to App1's managed identity grants Microsoft Entra ID-based read access to files and directories in Azure Files, overriding existing ACL restrictions where necessary. This allows the application to authenticate by using its managed identity instead of storage account keys.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-assign-share-level-permissions?tabs=azure-portal>

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Valid SC-500 Dumps shared by EduDump.com for Helping Passing SC-500 Exam! EduDump.com now offer the **newest SC-500 exam dumps**, the EduDump.com SC-500 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-500 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-500/premium/> (**136 Q&As** Dumps, **35%OFF** Special Discount Code: **freecram**)